

Annual 47 CFR § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 28, 2019
2. Name of company(s) covered by this certification: MIDCONTINENT COMMUNICATIONS
3. Form 499 Filer ID: 802284
4. Name of signatory: Patrick J. Mastel
5. Title of signatory: General Counsel
6. Certification:

I, Patrick J. Mastel, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company *has not* taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company *has not* received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed  [Signature of an officer, as agent of the carrier]

**Attachments:**      Accompanying Statement explaining CPNI procedures  
                                 Explanation of actions taken against data brokers (if applicable)  
                                 Summary of customer complaints (if applicable)

## **OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES**

Midcontinent Communications (the “Company”) has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network information (CPNI), § 64.2001 through § 64.2011.

### **CPNI Compliance Officer**

The Company has appointed a CPNI Compliance Officer. The CPNI Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The CPNI Compliance Officer is also the point of contact for anyone (internally or externally) with questions regarding CPNI.

### **Employee Training**

The Company Training Department arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the Company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company’s procedures for protecting CPNI and they understand the Company’s CPNI disciplinary process for improper use of CPNI. Each employee is informed as to where the Company’s CPNI policy is kept.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Regulatory Department or the CPNI Compliance Officer immediately.

### **Marketing Campaigns**

The Company has established a supervisory review process for any direct marketing. The Vice President of Marketing will review the campaign and all materials to ensure that it complies with the CPNI rules.

### **Customer Notification and Request for Approval to Use CPNI**

The Company has not provided notification to its customers and has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval. The Company does not share customer CPNI with any joint venture partner, independent contractor or any other third party. For marketing purposes, the Company does mass market to all customers, or at times uses CPNI to market only service offerings among the categories of service to which the customer already subscribes.

If the Company received a call from a customer who wants to discuss services outside of the customer's existing service offerings, the customer service representative uses the oral notification of one-time use of CPNI to obtain approval for the duration of the call only.

### **Authentication**

The Company does not disclose or share any CPNI until the customer has been appropriately authenticated as follows:

**In-office visit** – the customer must provide a valid photo ID matching the customer's account information.

**Customer-initiated call** – the customer must verify their account information before any employee can provide comments or take requests for any account changes. At minimum, customers must provide their name, address and a password that has been established by the account holder.

If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, date and time of the call, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
- If the customer cannot provide all the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to visit one of the Customer Experience Centers and provide valid photo ID.

### **Notification of Account Changes**

The Company promptly notifies customers whenever a change is made to any of the following:

- Address of record
- Account passwords
- Online account changes

The notification to the customer will be sent to the address (postal or electronic) of record. The Company has a process for tracking when a notification is required and how the notification is made. The Company's software program generates the notification letter.

### **Notification of Breaches**

Employees will immediately notify the Regulatory Department and the CPNI Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the CPNI Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but no later than seven (7) business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify customers, only after seven (7) full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested extension.
- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.
- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

### **Annual Certification**

The CPNI Compliance Officer will ensure that a CPNI Compliance Certification is filed with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

### **Record Retention**

The Company retains all information regarding CPNI electronically. Following is the minimum retention period the Company established for specific items:

- CPNI notification and records of approval – two years
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years